SECTION II—REMARKS

Applicants thank the Examiner for a thorough review, and respectfully request reconsideration of the above referenced patent application for the following reasons:

Claims 1-16, 18-19 and 21-25 rejected under 35 U.S.C. § 103(a)

The Office Action rejected claims 1-16, 18-19 and 21-25 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 7,127,524 to Renda et al. ("Renda") in view of U.S. Patent 7,143,435 to Droms et al. ("Droms"). Applicants respectfully submit that claims 1-25 are canceled herein without prejudice, and thus, the rejection to claims 1-16, 18-19 and 21-25 is rendered moot. However, Applicants respectfully submit that new claims 26-44 presented herein are patentable over the prior art of record. For example, new independent claim 26 recites in pertinent part:

> … **issuing the computing device a first Internet Protocol (IP) address assigned to a first Virtual Local Area Network (VLAN)** communicably interfaced with the packet forwarder, the first VLAN isolated from a permanent VLAN that provides access to the network;
>
> sending … an authentication request …
>
> receiving authentication credentials …
>
> **issuing the computing device a replacement IP address assigned to the permanent VLAN** for communication with the network, responsive to receiving satisfactory authentication credentials from the computing device; and
>
> forwarding network packets … .

Brief description of the claimed limitations:

In an effort to expedite prosecution of the present application, Applicants provide a brief description of some novel elements of the claimed limitations.

Applicants teach in the specification as originally filed, systems and methods for improving network security while balancing secure access to the network with the need to accept connection requests from potentially unknown computing devices, such as laptops, cell phones, pocket PCs, and so forth, in an open computing environment, such as a University campus. For example, refer to, *inter alia*, paragraph 30 of Applicants' specification:

> **[0030]** The method and apparatus for network login authorization is suitable for operating in a variety of networked environments. One environment is the **"campus environment," where the typical user is a roaming user that connects to the network at various locations throughout the campus**. In the campus environment, the port through which the user connects is not assigned to a permanent VLAN (i.e. layer-2 domain) until the user is authorized through the network login authorization. … .

Applicants teach that traditional methods of protecting networks are, in some situations, potentially undesirable for several reasons. For example, one primary problem with traditional methods is that network security is dependent upon resources within the network to perform authentication routines before allowing access to such a resource. For example, a user within a network may attempt to access a protected server, and that server will require the user to authenticate before allowing access to its resources. However, the user, or the user's computing device, must already have **access to the network itself** before it can authenticate with the protected server. Thus, it is the protected server itself that is secure, and not the network. Although protection of computing resources on a network is beneficial, preventing unauthorized users from accessing the network in the first place may provide more robust security.

Consider for example, the following excerpt from Applicants' specification, teaching in pertinent part:

> **[0003]** … In the past, computer networks were mainly **private networks** contained within a private office. Now, however, an entire building with **multiple offices of different**

> **companies** may make up a single local area network (LAN), a user may use a laptop to access a wireless LAN in a public place, or a student may plug a laptop into network ports in various classrooms. Situations like these **open a network to potential cyber-attacks** that may compromise the security of network resources and also prevent access by legitimate users. … **Security mechanisms in the devices at the network edge, such as LAN switches, are particularly critical because they grant access to the rest of the network.**
>
> **[0004]** … Generally most [past] security techniques take place **between network nodes** (a node is an end point for data transmissions, such as a computer workstation, network server …) and **not between connection points** (a connection point is an intermediate point in the network, such as a router, hub, or a switch).

Thus, Applicants teach that allowing computing devices on to a network and performing authentication routines "between network nodes," such as a protected server **on the network**, leaves the network itself open to various cyber-attacks. Applicants teach that protecting the network itself from unauthorized access may provide improved security. Applicants further explain some negative implications of allowing a computing device access to the network, even if network resources are themselves protected. For example:

> **[0008]** A drawback to prior art login procedures is that a user who **plugs a computer into a network port has immediate access to the network**, although they may not necessarily have access to any of the resources on the network (i.e. they have not yet successfully completed the login procedure).

Applicants further teach that, although some mechanisms do exist for protecting access to the network itself, such methods are machine based, relying on a trusted relationship with a particular piece of hardware, rather than relying on user or account based credentials for access to the network. Network security that relies on a trusted relationship with a particular machine is subject to a complete breach if a non-authorized user gains access to a trusted machine. Furthermore, such security mechanisms are impractical in situations where the network is in an

open public setting, such as a University campus, where individual users may have authorization to access the network, but it is unknown, or impractical to know, whether or not a particular computing device employed by any given user is trusted. For example:

> **[0011]** A major drawback to access lists, DoS, and SYN attack protections is that **access to the network is machine- or hardware-based instead of user-based**. Therefore, an unauthorized user who has access to an authorized machine **can still gain access to the network**, completely bypassing the intended security protection. Moreover, publicly accessed network resources, e.g. a web server not protected by a firewall, are more susceptible since access to a public resource cannot usually be restricted to certain machines or IP addresses. … .

To overcome the various limitations discussed above, Applicants teach a novel method to establish communication with a computing device so that appropriate authentication routines may be performed, while at the same time, disallowing that computing device from gaining access to the protected network itself. For example, Applicants teach and claim that, responsive to a connection request from a computing device, a packet forwarder "issu[es] the computing device a **first Internet Protocol (IP) address** assigned to a first Virtual Local Area Network (VLAN) communicably interfaced with the packet forwarder." Using the first IP address on the first VLAN, the packet forwarder can communicate with the computing device, without subjecting the protected network to potential attack. For example, Applicants teach in pertinent part:

> **[0030]** … In the campus environment, the port through which the user connects **is not assigned to a permanent VLAN** (i.e. layer-2 domain) until the user is authorized through the network login authorization. … .
>
> **[0031]** … In both the campus and network provider environments, prior to authorization through network login authorization, the user **obtains a temporary layer-3 address in order to gain access to the authenticator discovery controller** 190, the network login controller 110, and user interface 120 on packet-forwarding device 200. … .

* * *

> [**0042**] FIG. 6 is a flow diagram illustrating certain aspects of a method to be performed by a computer executing authenticator discovery according to one embodiment of the invention. … In one embodiment, the **user device may need to obtain a temporary IP address** from an IP address server 130 accessible to packet forwarding device 200.

Applicants further teach and claim that, "responsive to receiving satisfactory authentication credentials from the computing device," the packet forwarder "issu[es] the computing device **a replacement IP address assigned to the permanent VLAN** for communication with the network." For example:

> [**0031**] … The **temporary layer-3 address is discarded upon successful authentication** through network login authorization, after which the user must **obtain another layer-3 address**, this time a permanent one, through an address server 130 **on the permanent VLAN** to which the port has been assigned … .

Thus, Applicants teach and claim a novel method for improving security on a protected network, while balancing the ability to operate in an open environment, where it is desirable to allow potentially unknown machines access to the network, subjected to appropriate authentication credentials.

Renda and Droms do not disclose the claimed limitations:

The Office Action rejected now canceled claim 1 as unpatentable over Renda in view of Droms. For example, the Office Action states that Droms discloses:

> In step 440, a **test is performed to determine whether the user is authorized to connect to the network**. For example, it is determined whether the response from the authentication and authorization server indicates that the user is **both authentic and authorized** to connect to the local network. If not, control passes to step 442 to block network traffic through that port and to send a message to the host that network access is rejected. [Refer to the Office Action at page 3, second paragraph citing Droms at column 14, lines 10-25].

Although Droms does disclose performing a test to "determine whether the user is authorized to **connect to the network**," Droms is silent with respect to "issuing the computing device a **first Internet Protocol (IP) address**" and "issuing the computing device **a replacement IP address** … responsive to receiving satisfactory authentication credentials," as Applicants recite in new independent claim 26.

More particularly, Droms fails to disclose that a second IP address, specifically the "replacement IP address" is issued to the computing device "**responsive to** receiving satisfactory authentication credentials," as claimed by Applicants.

Droms is further silent with regard to which Virtual Local Area Network (VLAN) the first IP address or the replacement IP address belong. For example, Applicants recite, "a first Internet Protocol (IP) address assigned to a **first Virtual Local Area Network (VLAN)** communicably interfaced with the packet forwarder," over which the packet forwarder "send[s] … an authentication request" to the computing device and "receiv[es] authentication credentials" from the computing device. Applicants further teach and claim, "a replacement IP address assigned to the **permanent VLAN** for communication with the network." Conversely, Droms provides no discussion with respect to the association between an IP address and a particular VLAN, be it the first IP address or the replacement IP address.

Renda does not cure the deficiencies of Droms as it too fails to disclose "issuing the computing device a **first Internet Protocol (IP) address**" and "issuing the computing device **a replacement IP address** … responsive to receiving satisfactory authentication credentials." Renda likewise fails to disclose any association between IP addresses and their respective VLANs as taught and claimed by Applicants.

Because Renda and Droms, whether considered alone or in combination, fail to disclose at least one limitation Applicants recite in new independent claim 26, Applicants respectfully submit that claim 26 is patentable over the references and in condition for allowance. Applicants further submit that independent claims 35 and 40, which recite similar limitations, as well as those claims depending on independent claims 26, 35 and 40, are patentable over the references and in condition for allowance.

Accordingly, Applicants respectfully request the Examiner to withdraw the rejection to claims 1-16, 18-19 and 21-25 and allow new claims 26-44.

New claims 26-44:

Applicants respectfully submit that new claims 26-44 are patentable over the prior art of record and in condition for allowance as discussed above with regard to the rejection under 35 U.S.C. § 103. Applicants further submit that new claims 26-44 find support in the specification as originally submitted and in the original claims.

Accordingly, Applicants respectfully request the Examiner to allow new claims 26-44.

CONCLUSION

Given the above amendments and accompanying remarks, all claims pending in the application are in condition for allowance. If the undersigned attorney has overlooked subject matter in any of the cited references that is relevant to allowance of the claims, the Examiner is requested to specifically point out where such subject matter may be found. Further, if there are any informalities or questions that can be addressed via telephone, the Examiner is encouraged to contact the undersigned attorney at (503) 439-8778.

Charge Deposit Account

Please charge our Deposit Account No. 02-2666 for any additional fee(s) that may be due in this matter, and please credit the same deposit account for any overpayment.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

/Gregory D. Caldwell/ Date: June 20, 2008
Gregory D. Caldwell
Registration No. 39,926
Attorney for Applicants

Blakely, Sokoloff, Taylor & Zafman LLP
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Telephone: (503) 439-8778
Facsimile: (503) 439-6073